Agency Information Security Plan Review Criteria

Agency		**Date submitted**	
Agency Contact		**Phone number**	
ESO Analyst		**Date reviewed**	

For each element of an agency information security plan required by the Information Security statewide policy #107-004-052 and Oregon Administrative Rule #125-800-0005 – 0020, indicate where the topic is covered by referencing the page number of the agency plan.

1. Processes to Identify Agency Information Assets	**Agency Plan page reference**	**ESO review**
Process(es) to identify agency information assets.		
Process(es) to identify information owners.		
Citation of governing legislation, regulations, policy compliance and/or contractual obligations that affect the management of the information (i.e., HIPAA, IRS regulations, agency-specific statute).		

ESO Analyst comments:

2. Processes Determine Information Sensitivity	**Agency Plan page reference**	**ESO review**
Process(es) to identify sensitivity of agency information assets.		
Process(es) for conducting impact assessments on the value of the assets and any risks associated with its disclosure. Assessment should include known legislation, regulations, policy compliance, and contractual obligations affecting the management or use of the information.		
Process(es) for classifying information assets based on criteria in the statewide Information Asset Classification policy #107-004-052.		

ESO Analyst comments:

3. Processes to Determine Appropriate Levels of Protection for Information	Agency Plan page reference	ESO review
Process(es) to determine appropriate levels of protection for information based on assigned classification.		

ESO Analyst comments:

4. Applicable Directives, Legal and Regulatory Requirements	Agency Plan page reference	ESO review
Identify directives and legal and regulatory requirements affecting the agency.		

ESO Analyst comments:

5. Identification of Information Security Roles and Responsibilities	**Agency Plan page reference**	**ESO review**
Identify roles and responsibilities for information security within the agency.		
Roles required by statewide policy: • Agency Director – responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. Also responsible for ensuring compliance with state enterprise security policies, standards, and security initiatives, and with state and federal regulations. • Information Security Officer – manages the agency information security program. Oversees compliance with policies and procedures regarding the security of information assets. • Information Owner – an individual or groups of individuals responsible to: ○ Create an initial information classification, including assigning classification levels to all data; ○ Approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management; ○ Ensure the information will be regularly reviewed for value and controls updated to manage risks due to new threats, vulnerabilities, or changes in the environment; ○ Perform periodic reclassification based on business impact analysis, changing business priorities and/or new laws, regulations and security standards; ○ Follow state archive documentation retention rules regarding proper disposition of all information assets. • Incident Response Point of Contact – responsible for communicating with State Incident Response Team and coordinating agency actions in response to an information security incident. • Users – responsible for complying with the provisions of policies, procedures and practices.		
Citation of governing legislation, regulations, policy compliance and/or contractual obligations that affect the management of the information (i.e., HIPAA, IRS regulations, agency-specific statute).		

ESO Analyst comments:

6. Identification of User Awareness and Training Elements	Agency Plan page reference	ESO review
Identify user security awareness and training elements as they apply to users (including employees, volunteers and contractors).		
Identify who must be trained and at what intervals.		

ESO Analyst comments:

7. Information Security Policies that Govern Information Security Activities	Agency Plan page reference	ESO review
Cite agency information security policies that govern agency information security activities, including policy name, number, and effective date.		
Where agency policies contain procedures that are required to be included in the agency information security plan, include copies of the policies as appendices to the plan document.		

ESO Analyst comments:

For each agency responsibility mandated by Oregon Revised Statute 182.122 and Oregon Administrative Rule #125-800-0005 – 0020, indicate where the topic is covered by referencing the page number of the agency plan.

1. Statutory Requirements	**Agency Plan page reference**	**ESO review**
Plan for conducting vulnerability, business risk, or compliance audits and communicate results to the DAS Enterprise Security Office.		
Plan/process for developing and implementing policies and		
Explicitly stated responsibility for information security and security of agency-owned systems, applications, desktops, LANs, etc.		
Plan for developing a capacity to respond to incidents, including implementation of forensic techniques, implementation of remedial actions, evaluation of lessons learned, and communication with the DAS Enterprise Security Office.		

ESO Analyst comments:

PLAN APPROVED:

____ ________________________

Theresa Masse, State Chief Information Security Officer *Date*